Joint Certification Program
Operations Support Solution
External Portal

Two-Factor Authentication Guide

Prepared by: New River Systems, Inc.

4/28/2023

Two-Factor Authentication Setup

All JCP Portal users, who have a username and password, will need to enable Two Factor Authentication (TFA) on their JCP Portal accounts. Two Factor Authentication (TFA) is a tool to help prevent unauthorized users from accessing your JCP Portal account.

How it works

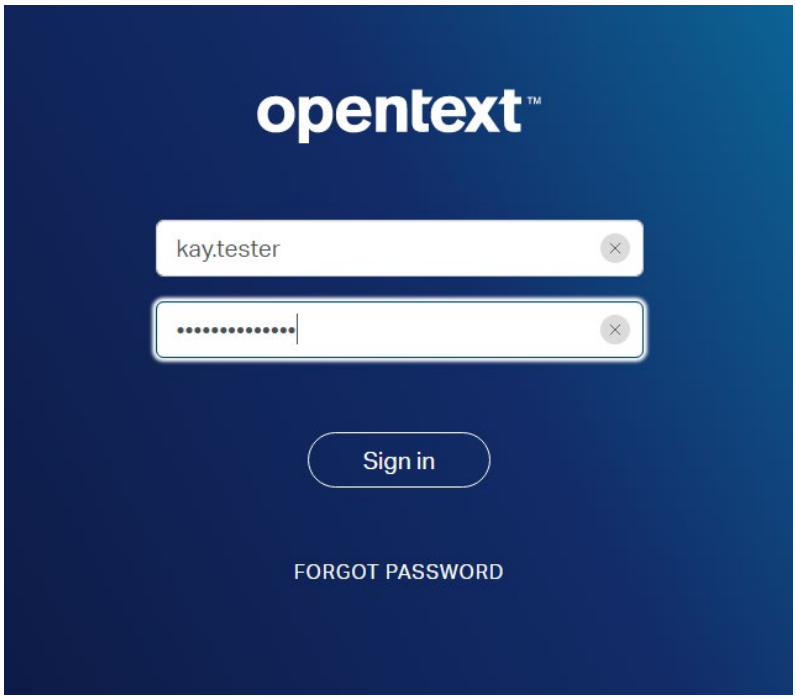
In a two-factor authentication system the first form of user identification is your current login credentials - your username and password. The second form of identification is created by a special algorithm in the JCP Portal system and sent to a device you have authorized to receive that code. JCP Portal is using a smartphone application, Google Authenticator, as the primary tool for receiving codes. Because any user attempting to login must possess both your username and password AND your phone, it is much more difficult for a user account to become compromised.

Google Authenticator app generates a six-digit code for you to enter when you log in. The code changes about every minute. Once you have set up the connection with JCP Portal's site, every time that you log out of your JCP Portal account you will need to use Google Authenticator to regain access when you login again.

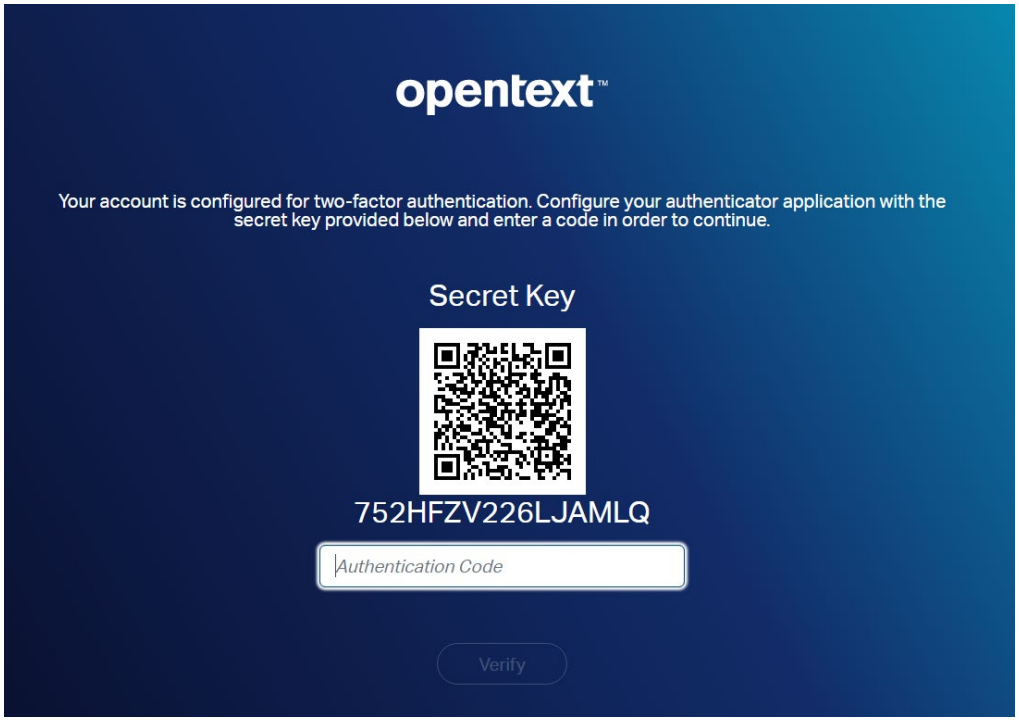
Steps to set up Google Authenticator

Follow the steps below to link Google Authenticator to your JCP Portal account and use it as your secondary method of identification.

- Login to your JCP Portal account using your username and password as you normally would.

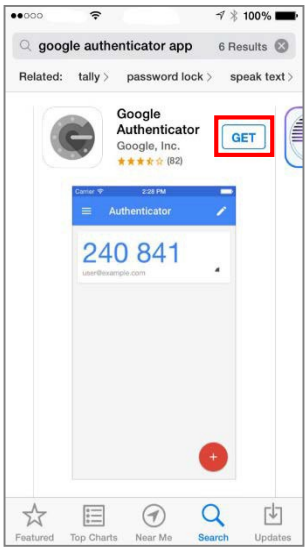


- On the next page, a prompt will inform you that you need to set up TFA on your account.
- On the next page, you will begin setup of Google Authenticator on your smartphone.
- You will be using Google Authenticator each time you login to JCP Portal to acquire the second authentication code the system now requires. Below that, you will see a manual verification code and a QR code you can scan with your phone.

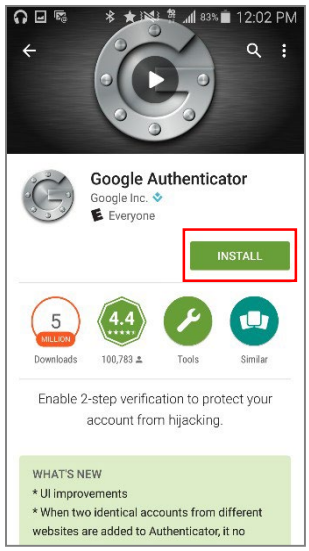


Browser screen showing the QR and manual authentication codes

- You will use these in the following steps to connect your smartphone app with your JCP Portal account.
- On your smartphone, open the App Store on your iPhone or the Google Play Store on your Android device. Search for “Google Authenticator.”
- The Google Authenticator app will appear as the top search result. In the App Store, select “Get” and then “Install”, as you do with any app you are installing. Choose the “Install” option in the Google Play Store.



iPhone App Store Screen

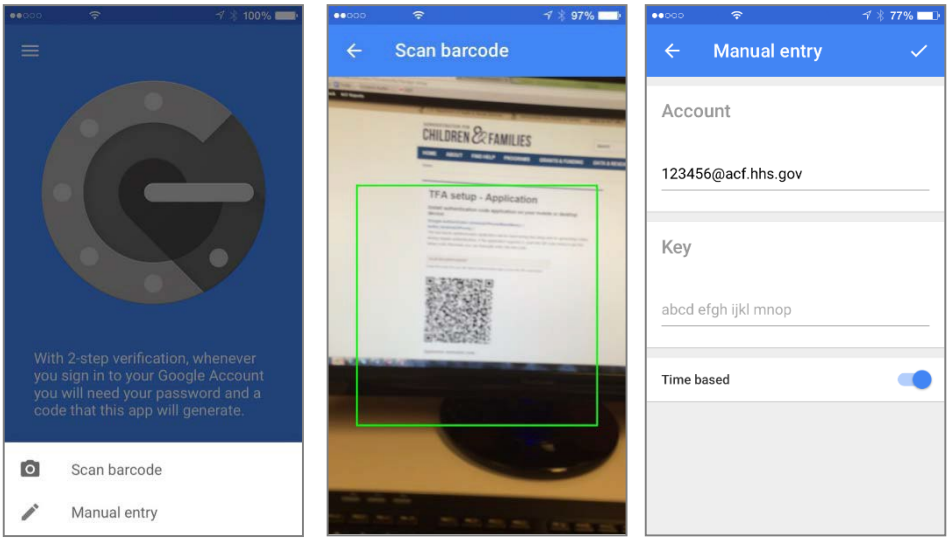


Google Play Store Screen

- **Note:** you may need to enter your App/Play Store password to verify that you want to download the application.
- Exit the app store and wait for the app to download before continuing. Once the Google Authenticator app has

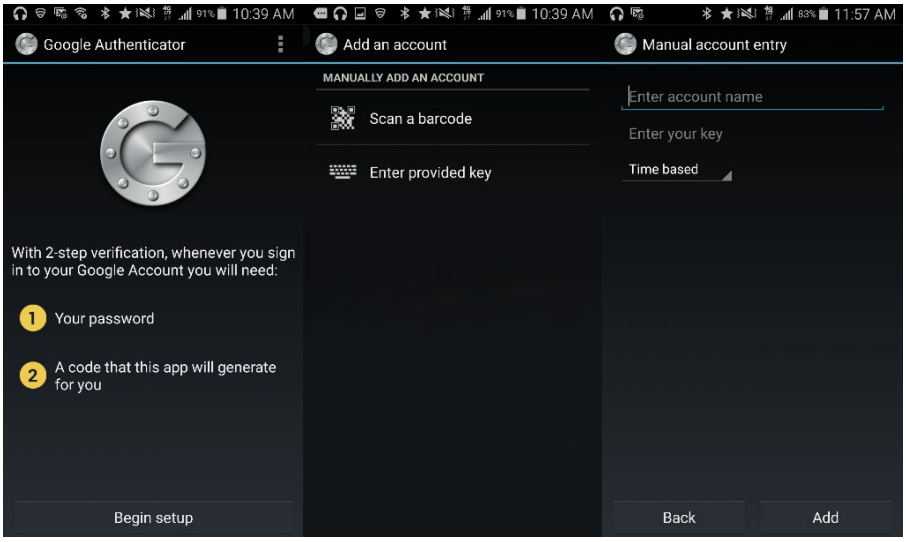
been installed, open the app.

- A menu will appear that will allow to you either scan the QR code on the JCP Portal or manually enter the verification code that appears above the QR code.



iPhone Screenshots from the Google Authenticator App

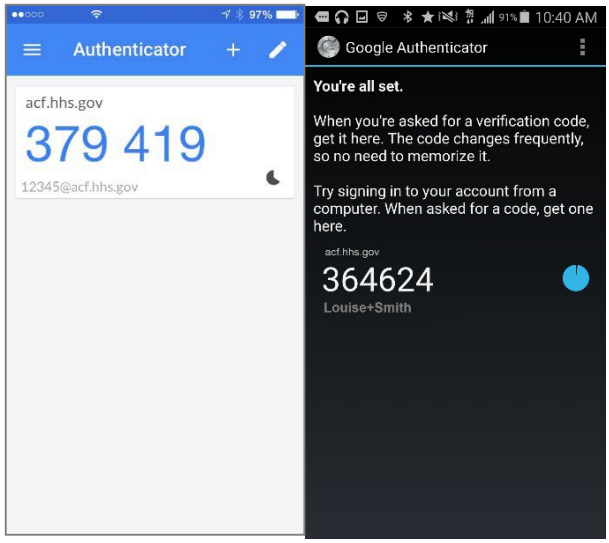
- **Note:** Android users should tap the “Begin Setup” button on the first screen in the application.



Android Screenshots from the Google Authenticator App

- If you select “Scan a barcode,” your phone’s camera will activate. Hold your phone close to the screen to allow the camera to capture the QR code.

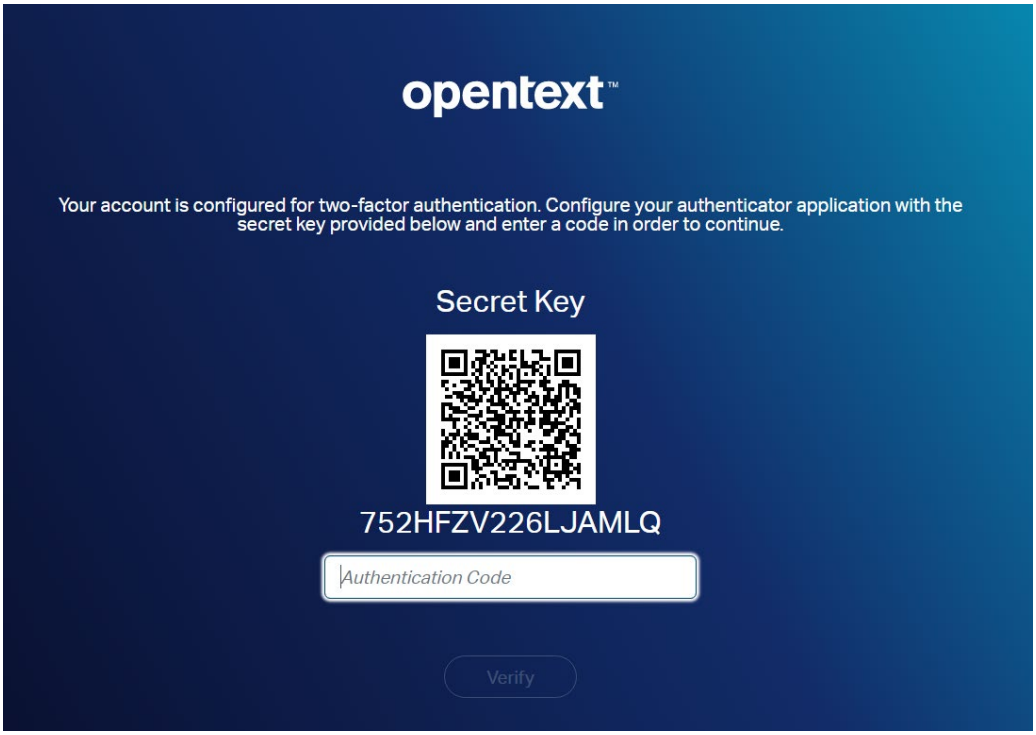
- When the QR code or manual code has processed, Google Authenticator will generate a six-digit verification code and display it.



iPhone Google Authenticator Code Screen

Android Google Authenticator Code Screen

- Type the six-digit code you see in the app into the JCP Portal below the QR code. Then select verify and save.
- **Note:** the code has a timer, if the timer expires you may need to enter in a new code before continuing your login.



The field in your Browser where you enter the initial Verification Code from the app